**Proprietary Back Doors**

Nonfree (proprietary) software is very often malware (designed to mistreat the user). Nonfree software is controlled by its developers, which puts them in a position of power over the users; [that is the basic injustice](https://www.gnu.org/philosophy/free-software-even-more-important.html). The developers and manufacturers often exercise that power to the detriment of the users they ought to serve.

This typically takes the form of malicious functionalities.

*Some malicious functionalities are mediated by*[*back doors*](https://www.gnu.org/proprietary/proprietary.html#f1)*. Here are examples of programs that contain one or several of those, classified according to what the back door is known to have the power to do. Back doors that allow full control over the programs which contain them are said to be “universal.”*

If you know of an example that ought to be in this page but isn't here, please write to [<webmasters@gnu.org>](mailto:webmasters@gnu.org) to inform us. Please include the URL of a trustworthy reference or two to serve as specific substantiation.

* [Spying](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#spy)

* [Altering user's data or settings](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#alter-data)

* [Installing, deleting or disabling programs](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#install-delete)

* [Full control](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#universal)

* [Other/undefined](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#other)

**Spying**

* Google Nest [is taking over ADT](https://blog.google/products/google-nest/partnership-adt-smarter-home-security/). Google sent out a software update to its speaker devices using their back door [that listens for things like smoke alarms](https://www.protocol.com/google-smart-speaker-alarm-adt) and then notifies your phone that an alarm is happening. This means the devices now listen for more than just their wake words. Google says the software update was sent our prematurely and on accident and Google was planning on disclosing this new feature and offering it to customers who pay for it.
* Many models of Internet-connected cameras contain a glaring back door—they have login accounts with hard-coded passwords, which can't be changed, and [there is no way to delete these accounts either](https://arstechnica.com/security/2017/06/internet-cameras-expose-private-video-feeds-and-remote-controls/).

Since these accounts with hard-coded passwords are impossible to delete, this problem is not merely an insecurity; it amounts to a back door that can be used by the manufacturer (and government) to spy on users.

* WhatsApp has a feature that [has been described as a “back door”](https://techcrunch.com/2017/01/13/encrypted-messaging-platform-whatsapp-denies-backdoor-claim/) because it would enable governments to nullify its encryption.

The developers say that it wasn't intended as a back door, and that may well be true. But that leaves the crucial question of whether it functions as one. Because the program is nonfree, we cannot check by studying it.

* Microsoft has [backdoored its disk encryption](https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key/).
* Apple can, and regularly does, [remotely extract some data from iPhones for the state](http://arstechnica.com/apple/2014/05/new-guidelines-outline-what-iphone-data-apple-can-give-to-police/).

This may have improved with [iOS 8 security improvements](https://www.denverpost.com/2014/09/17/apple-will-no-longer-unlock-most-iphones-ipads-for-police/); but [not as much as Apple claims](https://firstlook.org/theintercept/2014/09/22/apple-data/).

**Altering user's data or settings**

* BlizzCon 2019 imposed a [requirement to run a proprietary phone app](https://arstechnica.com/gaming/2019/05/blizzcon-2019-tickets-revolve-around-invasive-poorly-reviewed-smartphone-app/) to be allowed into the event.

This app is a spyware that can snoop on a lot of sensitive data, including user's location and contact list, and has [near-complete control](https://old.reddit.com/r/wow/comments/bkd5ew/you_need_to_have_a_phone_to_attend_blizzcon_this/emg38xv/) over the phone.

* Android has a [back door for remotely changing “user” settings](https://www.theverge.com/platform/amp/2018/9/14/17861150/google-battery-saver-android-9-pie-remote-settings-change).

The article suggests it might be a universal back door, but this isn't clear.

* The Dropbox app for Macintosh [takes control of user interface items after luring the user into entering an admin password](https://web.archive.org/web/20180124123506/http:/applehelpwriter.com/2016/07/28/revealing-dropboxs-dirty-little-security-hack/).
* A pregnancy test controller application not only can [spy on many sorts of data in the phone, and in server accounts, it can alter them too](http://www.theverge.com/2016/4/25/11503718/first-response-pregnancy-pro-test-bluetooth-app-security).
* [Some D-Link routers](http://www.itworld.com/article/2705284/backdoor-found-in-d-link-router-firmware-code.html) have a back door for changing settings in a dlink of an eye.

[The TP-Link router has a back door](http://sekurak.pl/tp-link-httptftp-backdoor/).

[Many models of routers have back doors](https://github.com/elvanderb/TCP-32764).

* Google has long had [a back door to remotely unlock an Android device](http://www.theguardian.com/technology/2015/nov/24/google-can-unlock-android-devices-remotely-if-phone-unencrypted), unless its disk is encrypted (possible since Android 5.0 Lollipop, but still not quite the default).
* Caterpillar vehicles come with [a back door to shutoff the engine](http://www.zerohedge.com/news/2015-11-19/caterpillar-depression-has-never-been-worse-it-has-cunning-plan-how-deal-it) remotely.
* Modern gratis game cr…apps [collect a wide range of data about their users and their users' friends and associates](http://toucharcade.com/2015/09/16/we-own-you-confessions-of-a-free-to-play-producer/).

Even nastier, they do it through ad networks that merge the data collected by various cr…apps and sites made by different companies.

They use this data to manipulate people to buy things, and hunt for “whales” who can be led to spend a lot of money. They also use a back door to manipulate the game play for specific players.

While the article describes gratis games, games that cost money can use the same tactics.

* [Samsung Galaxy devices running proprietary Android versions come with a back door](https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor) that provides remote access to the files stored on the device.
* The Amazon Kindle-Swindle has a back door that has been used to [remotely erase books](http://pogue.blogs.nytimes.com/2009/07/17/some-e-books-are-more-equal-than-others/). One of the books erased was *1984*, by George Orwell.

Amazon responded to criticism by saying it would delete books only following orders from the state. However, that policy didn't last. In 2012 it [wiped a user's Kindle-Swindle and deleted her account](http://boingboing.net/2012/10/22/kindle-user-claims-amazon-dele.html), then offered her kafkaesque “explanations.”

Do other ebook readers have back doors in their nonfree software? We don't know, and we have no way to find out. There is no reason to assume that they don't.

* The iPhone has a back door for [remote wipe](http://www.npr.org/2010/11/22/131511381/wipeout-when-your-company-kills-your-iphone). It's not always enabled, but users are led into enabling it without understanding.

**Installing, deleting or disabling programs**

* A very popular app found in the Google Play store contained a module that was designed to [secretly install malware on the user's computer](https://arstechnica.com/information-technology/2019/08/google-play-app-with-100-million-downloads-executed-secret-payloads/). The app developers regularly used it to make the computer download and execute any code they wanted.

This is a concrete example of what users are exposed to when they run nonfree apps. They can never be completely sure that a nonfree app is safe.

* Apple appears to say that [there is a back door in MacOS](https://techcrunch.com/2019/07/10/apple-silent-update-zoom-app/) for automatically updating some (all?) apps.

The specific change described in the article was not malicious—it protected users from surveillance by third parties—but that is a separate question.

* Corel Paintshop Pro has a [back door that can make it cease to function](https://torrentfreak.com/corel-wrongly-accuses-licensed-user-of-piracy-disables-software-remotely-181110/).

The article is full of confusions, errors and biases that we have an obligation to expose, given that we are making a link to them.

* + Getting a patent does not “enable” a company to do any particular thing in its products. What it does enable the company to do is sue other companies if they do some particular thing in their products.
  + A company's policies about when to attack users through a back door are beside the point. Inserting the back door is wrong in the first place, and using the back door is always wrong too. No software developer should have that power over users.
  + “[Piracy](https://www.gnu.org/philosophy/words-to-avoid.html#Piracy)” means attacking ships. Using that word to refer to sharing copies is a smear; please don't smear sharing.
  + The idea of “protecting our IP” is total confusion. The term “IP” itself is a [bogus generalization about things that have nothing in common](https://www.gnu.org/philosophy/not-ipr.html).

In addition, to speak of “protecting” that bogus generalization is a separate absurdity. It's like calling the cops because neighbors' kids are playing on your front yard, and saying that you're “protecting the boundary line”. The kids can't do harm to the boundary line, not even with a jackhammer, because it is an abstraction and can't be affected by physical action.

* Some “Smart” TVs automatically [load downgrades that install a surveillance app](https://web.archive.org/web/20180405014828/https:/twitter.com/buro9/status/980349887006076928).

We link to the article for the facts it presents. It is too bad that the article finishes by advocating the moral weakness of surrendering to Netflix. The Netflix app [is malware too](https://www.gnu.org/proprietary/malware-google.html#netflix-app-geolocation-drm).

* Baidu's proprietary Android library, Moplus, has a back door that [can “upload files” as well as forcibly install apps](https://www.eff.org/deeplinks/2015/11/millions-android-devices-vulnerable-remote-hijacking-baidu-wrote-code-google-made).

It is used by 14,000 Android applications.

* In addition to its [universal back door](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#windows-update), Windows 8 has a back door for [remotely deleting apps](https://www.computerworld.com/article/2500036/microsoft--we-can-remotely-delete-windows-8-apps.html).

You might well decide to let a security service that you trust remotely *deactivate* programs that it considers malicious. But there is no excuse for *deleting* the programs, and you should have the right to decide whom (if anyone) to trust in this way.

* In Android, [Google has a back door to remotely delete apps](https://www.computerworld.com/article/2506557/google-throws--kill-switch--on-android-phones.html). (It was in a program called GTalkService, which seems since then to have been merged into Google Play.)

Google can also [forcibly and remotely install apps](https://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/) through GTalkService. This is not equivalent to a universal back door, but permits various dirty tricks.

Although Google's *exercise* of this power has not been malicious so far, the point is that nobody should have such power, which could also be used maliciously. You might well decide to let a security service remotely *deactivate* programs that it considers malicious. But there is no excuse for allowing it to *delete* the programs, and you should have the right to decide who (if anyone) to trust in this way.

* The iPhone has a back door [that allows Apple to remotely delete apps](http://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html) which Apple considers “inappropriate”. Jobs said it's OK for Apple to have this power because of course we can trust Apple.

**Full control**

* BMW will remotely [enable and disable functionality in cars](https://www.cnet.com/roadshow/news/bmw-vehicle-as-a-platform/) through a universal back door.
* The [Google Play Terms of Service](https://www.google.com/mobile/android/market-tos.html) insist that the user of Android accept the presence of universal back doors in apps released by Google.

This does not tell us whether any of Google's apps currently contains a universal back door, but that is a secondary question. In moral terms, demanding that people accept in advance certain bad treatment is equivalent to actually doing it. Whatever condemnation the latter deserves, the former deserves the same.

* Android phones subsidized by the US government come with [preinstalled adware and a back door for forcing installation of apps](https://arstechnica.com/information-technology/2020/01/us-government-funded-android-phones-come-preinstalled-with-unremovable-malware/).

The adware is in a modified version of an essential system configuration app. The back door is a surreptitious addition to a program whose stated purpose is to be a [universal back door for firmware](https://www.zdnet.com/article/unremovable-malware-found-preinstalled-on-low-end-smartphone-sold-in-the-us/).

In other words, a program whose raison d'être is malicious has a secret secondary malicious purpose. All this is in addition to the malware of Android itself.

* The Chinese Communist Party's [“Study the Great Nation” app](https://www.gnu.org/proprietary/proprietary-surveillance.html#M201910130) was found to contain [a back-door allowing developers to run any code they wish](https://www.ndtv.com/world-news/chinese-app-allows-officials-access-to-100-million-users-phone-report-2115962) in the users' phone, as “superusers.”

Note: The [Washington Post version of the article](http://web-old.archive.org/web/20191015005153/https:/www.washingtonpost.com/world/asia_pacific/chinese-app-on-xis-ideology-allows-data-access-to-100-million-users-phones-report-says/2019/10/11/2d53bbae-eb4d-11e9-bafb-da248f8d5734_story.html) (partly obfuscated, but readable after copy-pasting in a text editor) includes a clarification saying that the tests were only performed on the Android version of the app, and that, according to Apple, “this kind of ‘superuser’ surveillance could not be conducted on Apple's operating system.”

* ChromeBooks are programmed for obsolescence: ChromeOS has a universal back door that is used for updates and [ceases to operate at a predefined date](https://www.theregister.co.uk/2019/08/22/buying_a_chromebook_dont_forget_to_check_when_it_expires/). From then on, there appears to be no support whatsoever for the computer.

In other words, when you stop getting screwed by the back door, you start getting screwed by the obsolescence.

* The FordPass Connect feature of some Ford vehicles has [near-complete access to the internal car network](https://www.myfordpass.com/content/ford_com/fp_app/en_us/termsprivacy.html). It is constantly connected to the cellular phone network and sends Ford a lot of data, including car location. This feature operates even when the ignition key is removed, and users report that they can't disable it.

If you own one of these cars, have you succeeded in breaking the connectivity by disconnecting the cellular modem, or wrapping the antenna in aluminum foil?

* New GM cars [offer the feature of a universal back door](https://media.gm.com/media/us/en/gmc/vehicles/canyon/2019.html).

Every nonfree program offers the user zero security against its developer. With this malfeature, GM has explicitly made things even worse.

* The Furby Connect has a [universal back door](https://www.contextis.com/blog/dont-feed-them-after-midnight-reverse-engineering-the-furby-connect). If the product as shipped doesn't act as a listening device, remote changes to the code could surely convert it into one.
* Sony has brought back its robotic pet Aibo, this time [with a universal back door, and tethered to a server that requires a subscription](https://motherboard.vice.com/en_us/article/bj778v/sony-wants-to-sell-you-a-subscription-to-a-robot-dog-aibo-90s-pet).
* Tesla used software to limit the part of the battery that was available to customers in some cars, and [a universal back door in the software](https://techcrunch.com/2017/09/09/tesla-flips-a-switch-to-increase-the-range-of-some-cars-in-florida-to-help-people-evacuate/) to temporarily increase this limit.

While remotely allowing car “owners” to use the whole battery capacity did not do them any harm, the same back door would permit Tesla (perhaps under the command of some government) to remotely order the car to use none of its battery. Or perhaps to drive its passenger to a torture prison.

* Vizio “smart” TVs [have a universal back door](https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen).
* Xiaomi phones come with [a universal back door in the application processor, for Xiaomi's use](https://web.archive.org/web/20190424082647/http:/blog.thijsbroenink.com/2016/09/xiaomis-analytics-app-reverse-engineered/).

This is separate from [the universal back door in the modem processor that the local phone company can use](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#universal-back-door-phone-modem).

* Microsoft Windows has a universal back door through which [any change whatsoever can be imposed on the users](http://www.informationweek.com/microsoft-updates-windows-without-user-permission-apologizes/d/d-id/1059183).

This was [reported in 2007](http://slated.org/windows_by_stealth_the_updates_you_dont_want) for XP and Vista, and it seems that Microsoft used the same method to push the [Windows 10 downgrade](https://www.gnu.org/proprietary/malware-microsoft.html#windows10-forcing) to computers running Windows 7 and 8.

In Windows 10, the universal back door is no longer hidden; all “upgrades” will be [forcibly and immediately imposed](http://arstechnica.com/information-technology/2015/07/windows-10-updates-to-be-automatic-and-mandatory-for-home-users/).

* The Amazon Echo appears to have a universal back door, since [it installs “updates” automatically](https://en.wikipedia.org/wiki/Amazon_Echo#Software_updates).

We have found nothing explicitly documenting the lack of any way to disable remote changes to the software, so we are not completely sure there isn't one, but this seems pretty clear.

* [A Chinese version of Android has a universal back door](http://www.theguardian.com/technology/2014/dec/18/chinese-android-phones-coolpad-hacker-backdoor). Nearly all models of mobile phones have a [universal back door in the modem chip](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#universal-back-door-phone-modem). So why did Coolpad bother to introduce another? Because this one is controlled by Coolpad.
* [Some applications come with MyFreeProxy, which is a universal back door](http://www.techienews.co.uk/973462/bitcoin-miners-bundled-pups-legitimate-applications-backed-eula/) that can download programs and run them.
* ChromeOS has a universal back door. At least, Google says it does—in [section 4 of the EULA](https://www.google.com/intl/en/chromebook/termsofservice.html).
* In addition to its [book eraser](https://www.gnu.org/proprietary/proprietary-back-doors.en.html#swindle-eraser), the Kindle-Swindle has a [universal back door](http://www.amazon.com/gp/help/customer/display.html?nodeId=200774090).
* Almost every phone's communication processor has a universal back door which is [often used to make a phone transmit all conversations it hears](https://www.schneier.com/blog/archives/2006/12/remotely_eavesd_1.html). See [Malware in Mobile Devices](https://www.gnu.org/proprietary/malware-mobiles.html#universal-back-door-phone-modem) for more info.

**Other or undefined**

* Intel's intentional “management engine” back door has [unintended back doors](https://www.theregister.co.uk/2017/11/20/intel_flags_firmware_flaws/) too.
* A Capcom's Street Fighter V update [installed a driver that could be used as a back door by any application installed on a Windows computer](https://www.theregister.co.uk/2016/09/23/capcom_street_fighter_v/), but was [immediately rolled back](https://www.rockpapershotgun.com/2016/09/24/street-fighter-v-removes-new-anti-crack) in response to public outcry.
* Dell computers, shipped with Windows, had a bogus root certificate that [allowed anyone (not just Dell) to remotely authorize any software to run](http://fossforce.com/2015/11/dell-comcast-intel-who-knows-who-else-are-out-to-get-you/) on the computer.
* ARRIS cable modem has a [back door in the back door](https://w00tsec.blogspot.de/2015/11/arris-cable-modem-has-backdoor-in.html?m=1).
* “Self-encrypting” disk drives do the encryption with proprietary firmware so you can't trust it. Western Digital's “My Passport” drives [have a back door](https://motherboard.vice.com/en_us/article/mgbmma/some-popular-self-encrypting-hard-drives-have-really-bad-encryption).
* Mac OS X had an [intentional local back door for 4 years](https://truesecdev.wordpress.com/2015/04/09/hidden-backdoor-api-to-root-privileges-in-apple-os-x/), which could be exploited by attackers to gain root privileges.
* Here is a big problem whose details are still secret: [The FBI asks lots of companies to put back doors in proprietary programs](http://mashable.com/2013/09/11/fbi-microsoft-bitlocker-backdoor/). We don't know of specific cases where this was done, but every proprietary program for encryption is a possibility.
* The German government [veers away from Windows 8 computers with TPM 2.0](https://www.theregister.co.uk/2013/08/23/nsa_germany_windows_8/) ([original article in German](https://www.zeit.de/digital/datenschutz/2013-08/trusted-computing-microsoft-windows-8-nsa)), due to potential back door capabilities of the TPM 2.0 chip.
* Here is a suspicion that we can't prove, but is worth thinking about: [Writable microcode for Intel and AMD microprocessors](https://web.archive.org/web/20150206003913/http:/www.afr.com/p/technology/intel_chips_could_be_nsa_key_to_ymrhS1HS1633gCWKt5tFtI) may be a vehicle for the NSA to invade computers, with the help of Microsoft, say respected security experts.
* HP “storage appliances” that use the proprietary “Left Hand” operating system have back doors that give HP [remote login access](https://insights.dice.com/2013/07/11/hp-keeps-installing-secret-backdoors-in-enterprise-storage/) to them. HP claims that this does not give HP access to the customer's data, but if the back door allows installation of software changes, a change could be installed that would give access to the customer's data.